



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,428	01/12/2001	Mitchell R. Frank	10004553-1	9973

22879 7590 07/22/2009

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER
----------

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2439

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

07/22/2009

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM  
ipa.mail@hp.com  
jessica.l.fusek@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

*Ex parte* MITCHELL R. FRANK, WILLIAM T. DANIELL,  
and BRIAN K. DAIGLE

---

Appeal 2009-000759  
Application 09/759,428  
Technology Center 2400

---

Decided:<sup>1</sup> July 20, 2009

---

Before JEAN R. HOMERE, JAY P. LUCAS, and JOHN A. JEFFERY,  
*Administrative Patent Judges.*

JEFFERY, *Administrative Patent Judge.*

DECISION ON APPEAL

---

<sup>1</sup> The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-28. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

### STATEMENT OF THE CASE

Appellants invented a system, method, and a computer-readable medium for locking down computer resources from vulnerabilities with a security application. The system and method involve an application that displays a list of security rules, permits selecting a rule, and displays information (e.g., benefits or consequences) about the selected rule. The information enables a system administrator to make better choices when defining the security profile.<sup>2</sup> Independent claim 1 is reproduced below with the key disputed limitations emphasized:

1. A computer system, comprising:

memory; and

a security application configured to display a list of *security rules* for locking down resources of said computer system, said security application configured to enable a set of said security rules, based on inputs from a user, and to cause said computer system to enforce said enabled set of security rules by modifying a machine state of said computer system, *said security application further configured* to enable said user to select one of said security rules and *to display information describing said selected rule in response to a selection of said one rule from said displayed list by said user*, said information based on data stored in said memory.

---

<sup>2</sup> See generally Spec. 1:14-20, 11:13-24, 13:11-14:8, 17:1-18; and 19:17-20:16; Figs. 2-3.

The Examiner relies upon the following as evidence in support of the rejection:

Deo	US 5,720,033	Feb. 17, 1998
Shrader	US 6,009,475	Dec. 28, 1999
Hayes, Jr.	US 6,339,826 B2	Jan. 15, 2002 (filed May 5, 1998)

(1) Claims 1-15, 23, and 28<sup>3</sup> stand rejected under 35 U.S.C. § 103(a) as being unpatentable by Hayes and Shrader. Ans. 3-6.

(2) Claims 16-22 and 24-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable by Hayes, Shrader, and Deo. Ans. 6-7.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer<sup>4</sup> for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

---

<sup>3</sup> The Examiner includes claims 24-27 in the obviousness rejection of Hayes and Shrader. However, claims 24-27 depend from claim 22, which is rejected as being unpatentable by Hayes, Shrader, and Deo. Accordingly, claims 24-27 should have been rejected with claim 22. Nevertheless, we deem the error harmless since the Examiner relies on the cited art (i.e., Hayes and Shrader) to reject claims 24-27. *See* Ans. 4-6.

<sup>4</sup> Throughout the opinion, we refer to: (1) the Appeal Brief filed July 10, 2006; (2) the Examiner's Answer mailed October 20, 2006; and (3) the Reply Brief filed December 15, 2006.

OBVIOUSNESS REJECTION OVER HAYES AND SHRADER

We group the claims as follows: (1) claims 1, 2, 8, and 28; (2) claim 3; (3) claims 9-11; (4) claims 4-6 and 12-15; (5) claim 7; and (6) claim 23. App. Br. 7-15 and 18. We address each grouping separately.

*(1) Claims 1, 2, 8, and 28*

Regarding representative independent claim 1,<sup>5</sup> the Examiner finds that Hayes discloses all the limitations of claim 1, except for the security application configured to enable the user to select one of the security rules and display information describing the rule in response to the selection. Ans. 3. The Examiner relies on Shrader to cure this deficiency. Ans. 3-4. Appellants argue that: (1) selecting Shrader's "actions" (e.g., push buttons shown in panes 220 and 250) does not suggest selecting of a security rule by the user; (2) the ticker tape pane 260 in Shrader updated in response to the "actions" or push buttons in panes 220 and 250 does not display information in response a selection of a security rule from a displayed list; and (3) there is motivation to combine Shrader with Hayes because Hayes has no apparent disadvantage that would cause an ordinarily skilled artisan to seek the benefits of Shrader. App. Br. 7-11; Reply Br. 2-4.

---

<sup>5</sup> While Appellants group claims 5 and 6 with claim 1 (App. Br. 7), claims 5 and 6 depend from claim 4. Claim 4 (App. Br. 14-15) has been argued separately, and claims 5 and 6 will be grouped accordingly. Claims 19 and 20 are rejected based on Hayes, Shrader, and Deo and will be separately addressed. As claims 2, 8, and 28 are not separately argued (App. Br. 7-18), we select independent claim 1 as representative. 37 C.F.R. § 41.37(c)(1)(vii).

## ISSUES

The following issues have been raised in the present appeal:

(1) Under § 103, have Appellants shown that the Examiner erred in rejecting claim 1 by finding that the combination of Hayes and Shrader teaches a security application that displays a lists of security rules?

(2) Under § 103, have Appellants shown that the Examiner erred in rejecting claim 1 by finding that Hayes and Shrader collectively teach the security application is configured to display information describing the rule in response to the user selecting one of the rules from the displayed list?

(3) Under § 103, have Appellants shown that the Examiner erred in finding a motivation to combine Shrader with Hayes to teach displaying information describing the selected rule in response to a selection of one of the rules from a display list in rejecting claim 1?

## FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

### *Hayes*

1. Hayes discloses a screenshot of a list 1720 under the Applet Permission tab 1518. The list 1720 includes permission status (i.e., deny or permit) and an applet name (e.g., TFTP, NFS, Log/Trace Facility) for various applets. Hayes includes a box entitled “Show Permitted Applets Only” located immediately above the Run/Customize button 1734. Col. 19, l. 50 – col. 20, l. 3; Fig. 17.

2. Hayes discusses that the administrator can change the permission status of an applet by selecting the applet and using the “Permit group access” and “Deny group access” buttons 1730 and 1732. Col. 19, l. 67 – col. 20, l. 3; Fig. 17.

*Shrader*

3. Shrader teaches an IP Filter Definition Page that includes a navigation pane 200 having a display pane 210 with a “Rule Action” drop-down lists 218. The drop-down lists 218 allows an administrator to define or modify filter entries. Col. 5, ll. 24-38 and col. 6, ll. 31-33; Fig. 4.

4. When the Rule Action “permit” is selected from the drop-down lists 218, permit filter entries are displayed in list pane 240 as a scrollable list of all filters defined for the Internet firewall. For example, entry #1 includes the description “permit 0 0 0 0 all any 0 any 0 both local both active # comment.” Col. 5, ll. 35-38 and 47-54 and col. 6, ll. 31-36; Fig. 4.

5. Shrader teaches previous administrator interfaces required memorization of many commands. Shrader’s invention is a user friendly interface for the administration of IP filtering on an Internet firewall. Col. 1, ll. 16-33.

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073-74 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966) (stating that 35 U.S.C.

§ 103 leads to three basic factual inquiries: the scope and content of the prior art, the differences between the prior art and the claims at issue, and the level of ordinary skill in the art). “[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.” *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). Furthermore, “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness . . . .” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

## ANALYSIS

Based on the record before us, we find no error in the Examiner’s obviousness rejection of claim 1. At the outset, we note that the Specification has no special definition for the term “security rule.” Thus, this phrase will be given its broadest reasonable construction “in light of the specification as it would be interpreted by one of ordinary skill in the art.” *In re Am. Acad. Of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citations and internal quotation marks omitted).

Hayes discloses a window that displays an applet list 1720 under the Applet Permission tab 1518. FF 1. This list 1720 includes information, such as the permission status (i.e., deny or permit) and the applet name (e.g., TFTP, NFS, Log/Trace Facility). *Id.* Hayes also discloses that the administrator has the ability to view only the permitted applets by selected the box immediately above the Run/Customize button 1734. *See id.* Further, each of these viewing options can be considered a different security rule. That is, the “permit and deny applets” viewing option shows



information about the “permit and deny” security rule and the “permitted applets” viewing option shows information about the “permitted” security rule. Thus, Hayes discloses a security application that provides different information based on the security rule the administrator selects.

Nonetheless, as the Examiner admits (Ans. 3), Hayes does not teach the security application displays information describing the selected rule in response to the selection of one of the rules from the displayed list. Shrader teaches an alternative navigation pane or window 200 that includes a display pane or window 210 having “Rule Action” drop-down lists 218. FF 3. Specifically, Shrader teaches the “permit” option of the drop-down lists 218 in Figure 4 that displays filters defined for the IP firewall. FF 4. As explained above, this “permit” option can be considered a security rule as broadly as recited.

Moreover, while only one type of security rule (e.g., “permit”) is shown in the drop down lists 218, Shrader states the “Rule Action” box includes drop-down lists. FF 3. Thus, Shrader teaches other “Rule Action” options (e.g., security rules) exist. Based on Hayes’ teachings that the administrator can alternatively display the “permit and deny” rule or the “permitted” rule (*see* FF 1), one skilled in the art would have recognized that Shrader’s drop-down lists 218 would also include other security rules, including a “permit and deny” rule that displays both permit and deny filters for the IP firewall. This combined Hayes and Shrader system provides the administrator with an alternative way of viewing the security rules using a drop-down list so as to define and modify filter entries. *See* FF 2 and 3. Therefore, regardless of whether the push buttons 220 and 250 in Shrader are security rules (App. Br. 8-9), the combined Hayes and Shrader system

teaches a security application configured to enable a user to select one security rule (e.g., “permit” rule or “permit and deny” rule) from a list of security rules (e.g., provided by the drop-down list 218) as required by claim 1.

Additionally, Shrader teaches a list pane or window 240 that presents a scrollable list of all the filters defined for the Internet firewall. FF 4. Thus, when the user selects the “Rule Action” permit or the “permit” security rule from the drop-down lists 218, all the permit filter entries with descriptions or information about the permitted filter (e.g., entry #1 includes the description “permit 0 0 0 0 all any 0 any 0 both local both active # comment”) will appear in list pane 240. *See id.* Likewise, when another rule is selected from the drop-down lists 218 (e.g., “permit and deny”), other information describing all the “permit” and “deny” filter entries will be displayed in response to the selection. Therefore, contrary to Appellants’ assertion (App. Br. 9-10), Shrader’s disclosure combined with Hayes teaches a “security application further configured . . . to display information describing said selected rule in response to a selection of said one rule from said displayed list by said user” as recited in claim 1.

Moreover, Shrader teaches an alternative arrangement for displaying security rule information and provides the administrator with a more user friendly interface, such as the drop-down lists over the numerous tabs or boxes of Hayes. *See* FF 1, 2, and 6. Based on Shrader’s teachings, one skilled in the art would have recognized Shrader’s interface would have improved Hayes’ layout by being more user friendly to an administrator. *See KSR*, 550 U.S. at 417. Additionally, Hayes only describes an applet’s name, while Shrader teaches providing more detailed information about

filter entries. *See* FF 1 and 4. Shrader suggests that the more information provided to the administrator the less memorization required. *See* FF 6. Thus, one skilled in the art would have similarly recognized Shrader's interface would have improved Hayes' layout by providing more detailed information and requiring less memorization for the administrator. *See KSR*, 550 U.S. at 417. Thus, contrary to Appellants' contentions (App. Br. 11), Shrader provides sufficient motivation to combine itself with Hayes in order to improve the security interface for the administrator and to minimize memorization.

For the foregoing reasons, Appellants have not shown the Examiner erred in rejecting claims 1, 2, 8, and 28 under 35 U.S.C. § 103 based on Hayes and Shrader.

*(2) Claim 3*

Claim 3<sup>6</sup> recites the security application in configured to display the list within a window having selectable icons and to display different sets of information describing the selected rule in response to the selections of different ones of the icons. The Examiner finds that Hayes discloses a plurality of icons (i.e., Members, Subgroups, and Applet Permission tabs) and that different information describing the selected rule is shown in response to the selected icon. Ans. 4. Appellants refer to the arguments made in connection with claim 1. App. Br. 12; Reply Br. 4. Appellants also argue only Hayes' Applet Permission tab displays information describing an

---

<sup>6</sup> Appellants group claim 7 with claim 3. App. Br. 12-13. However, claim 7 depends indirectly from claim 4. Because claim 4 was separately argued, we group claim 7 with claim 4. 37 C.F.R. § 41.37(c)(1)(vii).

alleged security rule, and, thus, the combination fails to teach a security application that displays different information describing the selected rule in response to the selection of different icons. App. Br. 12-13; Reply Br. 4.

#### ADDITIONAL ISSUE

The following additional issues have been raised in the present appeal:

(4) Under § 103, have Appellants shown that the Examiner erred in rejecting claim 3 by finding that Hayes and Shrader collectively teach a security application having a window with a plurality of icons and different information describing the selected rule is displayed in response to the selected icon?

#### ADDITIONAL FINDINGS OF FACT

The record supports the following additional findings of fact (FF) by a preponderance of the evidence.

##### *Hayes*

6. Hayes discloses a Members tab 1514, a Subgroups tab 1516, and an Applet Permission tab 1518. The Members tab 1514 shows a list 1520 of log-on identifications of all members that are defined to the system. The Subgroups tab shows a list 1620 of all immediate subgroups of “AllUsers” group. Col. 19, l. 8-10 and 28-32; Figs. 15-17.

#### ANALYSIS

Based on the record before us, we find no error in the Examiner’s obviousness rejection of claim 3. First, the Specification has no definition of the term “icon.” Thus, we will be giving this term its broadest reasonable

interpretation. *Am. Acad. Of Sci.*, 367 F.3d at 1364. We agree with Appellants that the Hayes' Member and Subgroups tabs or icons 1514 and 1516 do not display different sets of information *describing the selected rule* in response to the icon selection. *See* FF 6. Nonetheless, Hayes' Member and Subgroups are icons. Additionally, we find that the text of the "Member" and "Subgroups" tabs in Hayes are graphical symbols or icons. Similarly, Shrader teaches various text, graphical symbols, or icons (e.g., "permit" option) are listed as part of the "Rule Action" drop-down lists 218. Thus, Shrader also discloses a window that displays a list and the list includes a plurality of text options or icons that displays different information once selected. That is, when the administrator selects a "Rule Action," such as "permit," information about the filter entries relating to the "permit" security rule are shown. *See* FF 3 and 4. Moreover, as explained above, when Shrader is combined with Hayes, the combined system would also include at least two icons (i.e., "permit" and "permit and deny") in the drop-down lists 218 that displays different information describing filter entries relating the "permit" or the "permit and deny" security rule. Thus, the combined Hayes and Shrader system further teaches a window that includes a plurality of icons configured to display different sets of information describing the selected rules as claim 3 requires.

For the foregoing reasons, Appellants have not shown the Examiner erred in rejecting claim 3 under 35 U.S.C. § 103 based on Hayes and Shrader.

*(3) Claims 9-11*

Representative independent claim 9<sup>7</sup> recites a method for locking down resources of computer systems including displaying a list of security rules for locking down resources of the computer system, selecting one of the security rules from the list, and displaying information describing the rule in response to the selection. Appellants refer to the arguments made in connection with claims 1. App. Br. 13; Reply Br. 4. The issues for claim 9 are, therefore, the same as those in connection with claim 1, and we are not persuaded that Hayes and Shrader fail to teach the limitations of claim 9. For the foregoing reasons, we will sustain the rejection of claim 9 and dependent claims 10 and 11 which fall with claim 9.

*(4) Claims 4-6 and 12-15*

Representative claim 4<sup>8</sup> recites the security application is configured to display rules of said list in a first sub-window and displays the information describing the rule in a second sub-window. The Examiner finds that Hayes discloses a main window in Figure 17, a first sub-window as the Members window, and the second sub-window as the Applet

---

<sup>7</sup> While Appellants group claims 13-15 with this argument (App. Br. 13), these claims depend from separately argued claim 12 and will be grouped accordingly. We select independent claim 9 as representative of the group comprising claims 9-11. 37 C.F.R. § 41.37(c)(1)(vii).

<sup>8</sup> Appellants group claim 12 with claim 4. App. Br. 14-15. Claims 5 and 6 are grouped with claim 1 (App. Br. 7), but depend directly or indirectly from claim 4. Also, appellants group claims 13-15 with claim 9. App. Br. 13. However, claims 13-15 depend directly or indirectly from claim 12. Accordingly, we select claim 4 as representative of the group comprising claims 4-6 and 12-15. 37 C.F.R. § 41.37(c)(1)(vii).

Permission window. Ans. 4. Appellants refer to the arguments made in connection with claims 1 and 9. App. Br. 14; Reply Br. 5. The issues for claim 4 are, therefore, the same as those in connection with claims 1 and 9. For the reasons previously discussed with regard to claims 1 and 9, we are not persuaded that Hayes and Shrader fail to teach the limitation of claim 4.

Citing to column 19, lines 8-10 and 50-55 in Hayes, Appellants also argue that the selection of the Members and the Applet Permission icons are displayed on the same window and do not appear on different sub-windows. App. Br. 14-15. The issue before us, then, is whether the combination of Hayes and Shrader teaches the limitation of a first sub-window to display rules of the list and a second sub-window to display a description of the selected rule as required by claim 4. As explained above in connection with claim 1, the combined Hayes and Shrader system teaches a window having first pane or sub-window 210 that displays security rules (e.g., “permit” security rule) and a second pane or sub-window 240 that describes the selected rule (e.g., “permit 0 0 0 0 all any 0 any 0 both local both active # comment”). FF 3-4. Thus, contrary to Appellants’ assertions (App. Br. 15), the combined Hayes and Shrader system teaches all the limitations of claim 4.

For the foregoing reasons, we will sustain the rejection of claim 4, and claims 5, 6, and 12-15 which fall with claim 4.

*(5) Claim 7*

Claim 7 depends from claim 6 but recites similar limitations to claim 3. For the reasons discussed above with regard to claim 3, we will sustain the rejection of claim 7.

*(6) Claim 23*

Claim 23 calls for a computer readable medium having logic for displaying a list of security rules, logic for enabling a user to make a selection of one of the security rules while the security rules list, including the one security rule, is being displayed, and logic for displaying information describing the selected rule in response to the selection. Appellants refer to the arguments made in connection with claim 1. App. Br. 17; Reply Br. 5. The issues for claim 23 are, therefore, the same as those in connection with claim 1, and we are not persuaded that Hayes and Shrader fail to teach the limitation of claim 23 for the reasons previously discussed with regard to claim 1. For the foregoing reasons, we will sustain the rejection of claim 23.

REJECTION OVER HAYES, SHRADER, AND DEO

We group the claims as follows: (1) claims 16-22 and (2) claims 24-27.



*Claims 16-22*

Representative claim 22<sup>9</sup> recites that the security application is configured to display simultaneously the first and second sub-windows. The Examiner finds that neither Hayes nor Shrader teaches displaying rules in a first sub-window and relies on Deo for this feature. Ans. 6-7. Appellants refer to the arguments made in connection with claim 4. App. Br. 16. We are not persuaded for the reasons previously discussed with regard to claim 4. Additionally, Appellants contend that Deo does not cure the alleged deficiencies of Hayes and Shrader, and that there is no motivation to combine Deo with Hayes and Shrader. App. Br. 16-17.

ADDITONAL ISSUE

The following additional issue has been raised in the present appeal:

(5) Under § 103, have Appellants shown that the Examiner erred in finding that the combination of Hayes, Shrader, and Deo teaches a security application configured to simultaneously display the first and second sub-windows in rejecting claim 22?

---

<sup>9</sup> Appellants group claims 18, 21, and 22. App. Br. 15-17. Claims 19 and 20 are grouped with claim 1 but are rejected using an additional reference, Deo. Ans. 6-7. Similarly, claims 16 and 17 are grouped with claim 9 but are also rejected using Deo. Ans. 6-7. Accordingly, we select claim 22 as representative. 37 C.F.R. § 41.37(c)(1)(vii).

## ANALYSIS

Based on the record before us, we find no error in the Examiner's rejection of claim 22. As discussed in connection with claim 4 above, the combined Hayes and Shrader system teaches a security application that includes a first sub-window 210 that displays a list of security rules in the drop-down lists 218 and a second sub-window 240 that describes the selected rule. FF 3-4. For example, when the "permit" security rule is selected from the drop-down list 218 of a first sub-window 210, information, such as "permit 0 0 0 0 all any 0 any 0 both local both active # comment," is displayed in the second sub-window 240. FF 4. Thus, Shrader teaches a security application configured to display simultaneously the first sub-window 210 with the list of security rules 218 and the second sub-window 240 having the information describing the rule as required by claim 22. *See* FF 3-4. We find, therefore, that Deo is cumulative.

For the foregoing reasons, Appellants have not shown the Examiner erred in rejecting claim 16-22 under 35 U.S.C. § 103 based on Hayes, Shrader, and Deo.

### *(2) Claims 24-27*

As for representative claim 24,<sup>10</sup> Appellants refer to the arguments made in connection with claims 1, 4, and 22. App. Br. 18; Reply Br. 5. The issues for claims 24-27 are, therefore, the same as those in connection with claims 1, 4, and 22. We are not persuaded that Hayes, Shrader, and Deo fail

---

<sup>10</sup> Appellants group claims 24-27. App. Br. 18. Accordingly, we select claim 24 as representative. 37 C.F.R. § 41.37(c)(1)(vii).

to teach the limitation of claims 24-27 because of the reasons previously discussed with regard to claims 1, 4, and 22. For the foregoing reasons, we will sustain the rejection of claims 24-27.

### CONCLUSIONS

(1) Under § 103, Appellants have not shown that the Examiner erred in rejecting claim 1 by finding that the combination of Hayes and Shrader teaches a security application that displays a lists of security rules for locking down resources of a computer system.

(2) Under § 103, Appellants have not shown that the Examiner erred in rejecting claim 1 by finding that Hayes and Shrader collectively teach the security application is configured to display information describing the rule in response to the user selecting one of the rules from the displayed list.

(3) Under § 103, Appellants have not shown that the Examiner erred in finding a motivation to combine Shrader with Hayes to teach displaying information describing the selected rule in response to a selection of one of the rules from a display list in rejecting claim 1.

(4) Under § 103, Appellants have shown that the Examiner erred in rejecting claims 3 and 7 by finding that Hayes and Shrader collectively teach a security application having a window with a plurality of icons and different information describing the selected rule is displayed in response to the selected icon.

(5) Under § 103, Appellants have not shown that the Examiner erred in finding that the combination of Hayes, Shrader, and Deo teaches a security application configured to simultaneously display the first and second sub-windows in rejecting claims 16-22.

#### DECISION

We have sustained the Examiner's rejection of claims 1-28. Accordingly, the Examiner's rejection of claims 1-28 is affirmed.

No period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

#### AFFIRMED

pgc

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS CO 80527-2400